ABSTRACT OF THE DISCLOSURE

Ring signature data that can be created with N public keys and a private key corresponding to one of the N public keys, that allows for signature verification for each of the N public keys, and that allows which one of N members has signed to be kept secret is input. Denial data, which allows for verification that a user other than the creator of the ring signature data has not signed, is created in accordance with the ring signature data. Whether a predetermined verification equation is satisfied is verified in accordance with the generated denial data. If it is satisfied, the user is proven not to be the creator. Thus, the user who has the private key for a public key used without authorization can prove that he or she has not signed.